FinCEN ADVISORY

FIN-2018-A007 **October 31, 2018**

Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies

On October 19, 2018, the Financial Action Task Force (FATF) updated its list of jurisdictions with strategic anti-money laundering and combatting the financing of terrorism (AML/CFT) deficiencies. The changes may affect U.S. financial institutions' obligations and risk-based approaches with respect to relevant jurisdictions.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to inform financial institutions of updates to the FATF list of jurisdictions with strategic AML/CFT deficiencies. Financial institutions should be aware of these changes, which may affect their obligations and risk-based approaches with respect to these jurisdictions. The advisory also reminds financial institutions of the status and obligations involving these jurisdictions, in particular the Democratic People's Republic of Korea (DPRK) and Iran.

As part of the FATF's listing and monitoring process to ensure compliance with its international AML/CFT standards, the FATF identifies certain jurisdictions as having strategic deficiencies in their AML/CFT regimes.[1] These jurisdictions are named in two documents: (1) the "FATF Public Statement," which identifies jurisdictions that are subject to the FATF's call for countermeasures and/or are subject to enhanced due diligence (EDD) because of their strategic AML/CFT deficiencies; and (2) "Improving Global AML/CFT Compliance: On-going Process," which identifies jurisdictions that the FATF has determined to have strategic AML/CFT deficiencies.[2] On October 19, 2018, the FATF updated both documents with the concurrence of the United States. Financial institutions should consider these changes when reviewing their obligations and risk-based policies, procedures, and practices with respect to the jurisdictions noted below.[3]

FATF "Public Statement":

- DPRK and Iran

1. The FATF (www.fatf-gafi.org) is a 37-member intergovernmental body that establishes international standards to combat money laundering and counter the financing of terrorism and proliferation of weapons of mass destruction. The United States is a member of the FATF.
2. The FATF public identification of countries with strategic AML/CFT deficiencies is in response to the G20 leaders' call for the FATF to reinvigorate its process for assessing countries' compliance with international AML/CFT standards. The G20 leaders have consistently called for the FATF to issue regular updates on jurisdictions with strategic deficiencies. Specifically, within the FATF, the International Cooperation Review Group (ICRG) monitors and identifies countries with AML/CFT deficiencies. For more information on the ICRG procedures, please visit the FATF's website.
3. *See* 31 U.S.C. §§ 5318(h) and (i).

FATF "Improving Global AML/CFT Compliance: On-going Process":

- Remaining on list: Ethiopia, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen
- Added to list: The Bahamas, Botswana, and Ghana

I. Jurisdictions That Are Subject to the FATF's Call for Countermeasures and/or Are Subject to EDD Due to Their Strategic AML/CFT Deficiencies

The FATF has stated that the following jurisdictions have strategic deficiencies in their AML/CFT regimes and has called upon its members and urged all jurisdictions to (1) impose countermeasures and/or (2) apply EDD proportionate to the risks arising from the jurisdiction.

Please click on each jurisdiction for additional information.

A. Countermeasures

DPRK

B. Enhanced Due Diligence

Iran

Review of Guidance Regarding the DPRK and Iran

DPRK

The FATF calls on its members and other countries to apply countermeasures against the DPRK to protect the international financial system from money laundering and terrorist financing risks. The FATF Public Statement on the DPRK emphasizes the high risk of proliferation financing attributable to the DPRK, consistent with United Nations Security Council resolutions (UNSCRs).[4] In particular, the FATF reaffirmed its call that jurisdictions close DPRK banks within their territories and terminate correspondent relationships with DPRK banks, as required by UNSCR 2270. Financial institutions should be acutely aware of the financial provisions and comprehensive prohibitions contained in the UNSCRs imposing sanctions on the DPRK.

Among other prohibitions and restrictions, UNSCR 2321, adopted in 2016, states that member states shall expel individuals acting on behalf of or at the direction of a bank or financial institution of the DPRK. UNSCR 2321 also expresses concern that individuals from the DPRK are sent abroad

4. Relevant UNSCRs include 2397 (December 2017), 2375 (September 2017), 2371 (August 2017), 2356 (June 2017), 2321 (November 2016), 2270 (March 2016), 2094 (March 2013), 2087 (January 2013), 1874 (June 2009), and 1718 (October 2006). *See* the United Nations Security Council Resolutions web page for more information.

to earn hard currency to fund the DPRK's nuclear and ballistic missile programs, and it reiterates the concern that the DPRK may use bulk cash to evade United Nations (UN) measures. UNSCR 2321 instructed member states to close existing representative offices, subsidiaries, or banking accounts in the DPRK within 90 days of the adoption of the resolution (unless individually exempted by the 1718 Committee), and states that member states shall prohibit public and private financial support within their territories or by persons or entities subject to their jurisdiction for trade with the DPRK.

In addition to UN sanctions, the U.S. Department of the Treasury's (Treasury) Office of Foreign Assets Control (OFAC) maintains a robust sanctions program on North Korea[5] through the North Korea Sanctions Regulations, 31 C.F.R. part 510, which implements DPRK-related Executive Orders (E.O.) 13466, 13551, 13570, 13687, 13722, and 13810; the North Korea Sanctions and Policy Enhancement Act of 2016 (NKSPEA); and relevant provisions of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA).[6] Separately, under the Weapons of Mass Destruction Proliferators Sanctions Regulations,[7] issued pursuant to E.O. 13382, OFAC administers sanctions on individuals and entities responsible for the proliferation of weapons of mass destruction (WMD), as well as their supporters, some of whom are North Korean or tied to North Korea and North Korean-related activity.[8] Collectively, these authorities prohibit U.S. persons, including U.S. financial institutions, from engaging in nearly all transactions involving the DPRK.[9] These sanctions are a direct response to the DPRK's ongoing: development of WMD and their means of delivery; launching of intercontinental ballistic missiles; nuclear tests; human rights abuses and censorship; destructive, coercive cyber-related actions; involvement in money laundering, the counterfeiting of goods and currency, bulk cash smuggling, and narcotics trafficking; and continued violations of UNSCRs.[10]

5. The DPRK is also referred to as North Korea.

6. *See* Treasury's Resource Center for North Korea Sanctions, 22 U.S.C. § 9201 et seq., and Public Law 115-44.

7. *See* 31 CFR Part 544.

8. *See* Executive Order 13382 (June 29, 2005).

9. Further information about these sanctions is available at OFAC's Resource Center for DPRK Sanctions and the OFAC Recent Actions web page. OFAC's sanctions prohibit U.S. persons, including U.S. financial institutions, from engaging in most transactions involving the DPRK, the Government of North Korea, and the Korean Workers' Party. OFAC recently took a series of sanctions actions related to the DPRK, including actions pursuant to Executive Order 13551 on October 25, 2018; Executive Orders 13551 and 13687 on October 4, 2018; Executive Orders 13722 and 13810 on September 13, 2018; and Executive Order 13810 on September 6, 2018. OFAC also took sanctions actions related to the DPRK on August 21, 2018 and August 15, 2018, as well as additional sanctions actions on August 3, 2018, pursuant to Executive Orders 13687, 13382, and 13722. OFAC previously took sanctions actions related to the DPRK pursuant to Executive Orders 13810 and 13722 on February 23, 2018. OFAC also issued DPRK-related sanctions pursuant to Executive Orders 13687, 13722, and 13810 on January 24, 2018. OFAC took other DPRK-related sanctions actions pursuant to Executive Orders 13810 and 13722 on November 21, 2017. OFAC imposed other DPRK-related actions pursuant to Executive Orders 13687 and 13722 on October 26, 2017, Executive Order 13810 on September 26, 2017, and Executive Orders 13382 and 13722 on August 22, 2017. OFAC took other DPRK-related sanctions pursuant to one or more of these same authorities on December 26, 2017, June 29, 2017, June 1,2017, March 31, 2017, December 2, 2016, and September 26, 2016. On November 20, 2017, the United States designated the DPRK a state sponsor of terrorism.

10. *See* Executive Orders 13810 (September 20, 2017), 13687 (January 2, 2015), and 13551 (August 30, 2010).

U.S. financial institutions should be particularly aware of the extensive nature of the sanctions associated with E.O. 13810 (September 2017).[11] The E.O. provides the Secretary of the Treasury, in consultation with the Secretary of State, additional tools to disrupt a broad range of DPRK-related activity, to include North Korea's ability to fund its WMDs and ballistic missile programs. Specifically, E.O. 13810: (1) establishes several new designation criteria; (2) prohibits vessels and aircraft that have called or landed at a port or place in North Korea in the previous 180 days, and vessels that engaged in a ship-to-ship transfer with such a vessel in the previous 180 days, from entering the United States; (3) provides authority to block any funds transiting accounts with links to North Korea that come within the United States or in the possession of a United States person; and (4) provides authority to impose sanctions on a foreign financial institution (FFI) that knowingly conducts or facilitates on or after September 21, 2017 (i) any significant transaction on behalf of any person blocked under the DPRK-related E.O.s or persons blocked under E.O. 13382 for North Korea-related activities or (ii) any significant transaction in connection with trade with North Korea. The sanctions applicable to FFIs can be restrictions on correspondent or payable-through accounts or full blocking sanctions.[12]

Since the issuance of E.O. 13810, OFAC has designated entities and individuals involved in North Korea's illicit shipping and transportation activities, trading companies, and financial and banking representatives, and identified multiple vessels as blocked property.[13] On July 23, 2018, OFAC issued a joint advisory with the U.S. Department of State and the U.S. Department of Homeland Security to alert businesses, to include U.S. and foreign businesses, to the sanctions evasion tactics used by North Korea that could expose them – including manufacturers, buyers, and service providers – to supply chain sanctions compliance risks under U.S. or UN sanctions authorities.[14] Earlier, on February 23, 2018, with the U.S. Department of State and the U.S. Coast Guard, OFAC issued a North Korea Sanctions Advisory on sanctions risks related to North Korea's shipping practices, to alert persons globally of North Korea's deceptive shipping practices to evade U.S. and UN sanctions.[15]

Other Treasury actions underscore the serious risks that any financial activity involving the DPRK may facilitate WMD and ballistic missile activities. In November 2016, pursuant to Section 311 of the USA PATRIOT Act, FinCEN issued a final rule prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, North Korean banking institutions and requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against the use of such accounts to process transactions involving North Korean financial institutions.[16] FinCEN noted

11. *See* Treasury's Resource Center for September 21, 2017 actions relating to North Korea and Remarks by Secretary Mnuchin on President Trump's Executive Order on North Korea.
12. *See* OFAC's Frequently Asked Questions (FAQs).
13. *See* Executive Order 13810 (September 20, 2017).
14. *See* Treasury's Resource Center, "Publication of North Korea Supply Chain Advisory."
15. *See* Treasury's Press Release, "Treasury Announces Largest North Korean Sanctions Package Targeting 56 Shipping and Trading Companies and Vessels to Further Isolate Rogue Regime."
16. 31 C.F.R. § 1010.659.

that the North Korean government continues to use state-controlled financial institutions and front companies to conduct illicit international financial transactions, some of which support the proliferation of WMD and the development of ballistic missiles.[17]

In November 2017, FinCEN also prohibited U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, Bank of Dandong, and required those covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving Bank of Dandong.[18] In promulgating the regulation, FinCEN found that the Chinese bank has acted as a conduit for illicit North Korean financial activity to access the U.S. and international financial systems, including the facilitation of millions of dollars of transactions for companies involved in North Korea's WMD and ballistic missile programs. Further, FinCEN found that Bank of Dandong has also facilitated financial activity for North Korean entities designated by the United States and listed by the UN for proliferation of WMDs, as well as for front companies acting on their behalf.[19]

On November 2, 2017, FinCEN also issued an advisory to further alert financial institutions to schemes commonly used by North Korea to evade U.S. and UN sanctions, launder funds, and finance the North Korean regime's weapons programs.[20]

Iran

The FATF continues to call upon its members and urges all jurisdictions to apply enhanced due diligence measures to protect against the terrorist financing risk emanating from Iran and the threat this poses to the international financial system. In addition to other standard enhanced due diligence procedures, in its October 2018 statement, the FATF specifically highlighted the need for financial institutions to apply enhanced due diligence, including obtaining information on the reasons for intended transactions, to business relationships and transactions with Iranian persons. The FATF remains concerned with the terrorist financing risk emanating from Iran.[21]

In October 2018, the FATF expressed its disappointment that the majority of Iran's Action Plan is still incomplete, despite its deadlines expiring in January 2018. Iran must fully address its remaining action items, specifically: "(1) adequately criminalizing terrorist financing, including by removing the exemption for designated groups 'attempting to end foreign occupation, colonialism and racism';

17. *Ibid*.

18. 31 C.F.R. § 1010.660.

19. *Ibid*.

20. *See* FIN-2017-A008, "Advisory on North Korea's Use of the International Financial System" (November 2017). In addition, FinCEN has issued three other advisories relating to the DPRK: FIN-2013-A005, "Update on the Continuing Illicit Finance Threat Emanating from North Korea" (July 2013); FIN-2009-A002, "North Korea Government Agencies' and Front Companies' Involvement in Illicit Financial Activities" (June 2009); and FinCEN Advisory – Issue 40, "Guidance to Financial Institutions on the Provisions of Banking Services to North Korean Government Agencies and Associated Front Companies Engaged in Illicit Activities" (December 2005).

21. *See* FATF Public Statement (October 19, 2018).

(2) identifying and freezing terrorist assets in line with the relevant United Nations Security Council resolutions; (3) ensuring an adequate and enforceable customer due diligence regime; (4) ensuring the full independence of the Financial Intelligence Unit and requiring the submission of STRs [Suspicious Transaction Reports] for attempted transactions; (5) demonstrating how authorities are identifying and sanctioning unlicensed money/value transfer service providers; (6) ratifying and implementing the Palermo and TF [Terrorist Financing] Conventions and clarifying the capability to provide mutual legal assistance; (7) ensuring that financial institutions verify that wire transfers contain complete originator and beneficiary information; (8) establishing a broader range of penalties for violations of the ML [Money Laundering] offense; and (9) ensuring adequate legislation and procedures to provide for confiscation of property of corresponding value."[22]

"By February 2019, the FATF expects Iran to have brought into force the necessary legislation in line with FATF standards, or the FATF will take further steps to protect against the risks emanating from deficiencies in Iran's AML/CFT regime. The FATF also expects Iran to continue to progress with enabling regulations and other amendments. Iran will remain on the FATF Public Statement until the full Action Plan has been completed. Until Iran implements the measures required to address the deficiencies identified in the Action Plan, the FATF will remain concerned with the terrorist financing risk emanating from Iran and the threat this poses to the international financial system. The FATF, therefore, calls on its members and urges all jurisdictions to continue to advise their financial institutions to apply enhanced due diligence, including obtaining information on the reasons for intended transactions, to business relationships and transactions with natural and legal persons from Iran."[23]

Treasury has consistently underscored the risks of conducting business with entities associated with Iran. Iran continues to use deceptive tactics including front and shell companies to exploit markets in numerous countries to fund its nefarious activities. Iran's tactics include forging documents, obfuscating data, and hiding illicit activities under official cover of government entities, among many others. On October 11, 2018, FinCEN issued a comprehensive advisory outlining the deceptive practices the Iranian regime employs to access the financial system with the intention of furthering its illicit and malign activities.[24]

To combat Iran's malign activities, including its efforts to deceive the international business community, OFAC has issued 19 rounds of sanctions since February 2017, designating 168 Iran-related persons for a range of activities related to Iran's support for terrorism, ballistic missile

22. *Ibid*.

23. *Ibid*.

24. *See* FIN-2018-A006, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System" (October 2018). FinCEN has issued numerous advisories related to Iran. *See* FIN-2018-A004, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (September 2018); FIN-2018-A002, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (April 2018); FIN-2010-A008, "Update on the Continuing Illicit Finance Threat Emanating from Iran" (June 2010); FIN-2008-A002, "Guidance to Financial Institutions on the Continuing Money Laundering Threat Involving Illicit Iranian Activity" (March 2008); and FIN-2007-A001, "Guidance to Financial Institutions on the Increasing Money Laundering Threat Involving Illicit Iranian Activity" (October 2007).

program, WMD proliferation, cyberattacks, transnational criminal activity, censorship, and human rights abuses.[25] Most recently, on October 16, 2018, OFAC issued sanctions aimed at a network of individuals, financial institutions, and companies providing financial support to the Basij Resistance Force, a paramilitary force subordinate to Iran's Islamic Revolutionary Guard Corps and the Islamic Revolutionary Guard Corps-Qods Force. The network operates shell companies and has taken other measures to hide the ownership and control over a variety of multibillion-dollar business interests in the automotive, mining, metals, and banking sectors with connections to Iran.[26]

Additionally, financial institutions should be familiar with the requirements and prohibitions contained in UNSCR 2231 related to Iran.[27]

Iran remains on the FATF Public Statement.[28] FATF action to continue the suspension of countermeasures does not remove or alter any obligation of U.S. persons, including financial institutions, regarding a broad range of restrictions and prohibitions on engaging in transactions with or involving Iran given the large number of illicit finance risks associated with Iran, including money laundering, terrorist financing, human rights abuses, and the financing of Iran's ballistic missile program.

Review of Guidance on Section 312 Obligations Relating to the DPRK and Iran

Financial institutions must comply with the extensive U.S. restrictions and prohibitions against opening or maintaining any correspondent accounts, directly or indirectly, with foreign banks licensed by the DPRK or Iran.

25. On August 6, 2018, E.O. 13846 re-imposed certain sanctions with respect to Iran. This E.O. supports the United States' withdrawal from the Joint Comprehensive Plan of Action and the initial 90-day wind-down period. The 180-day wind-down period will end on November 4, 2018. Consult OFAC's FAQs concerning E.O. 13846 and the re-imposition of sanctions that occurred by August 6, 2018. In addition to sanctions re-imposed by E.O. 13846, OFAC issued Iran-related designations on October 16, 2018, September 14, 2018, July 9, 2018, May 30, 2018, May 24, 2018, May 22, 2018, May 17, 2018, May 15, 2018, May 10, 2018, March 23, 2018, January 12, 2018, January 4, 2018, November 20, 2017, and October 13, 2017. Furthermore, OFAC previously issued Iran-related designations associated with Iran's ballistic missile program on July 28, 2017, July 18, 2017 (in conjunction with those issued by the U.S. Department of State and in coordination with the U.S. Department of Justice's release of information involving a related criminal enforcement action), September 14, 2017, May 17, 2017, April 13, 2017, and February 3, 2017. Consult OFAC's Iran Sanctions web page and the OFAC Recent Actions web page for more detailed information about the sanctions included in this footnote.
26. *See* Treasury's Press Release "Treasury Sanctions Vast Financial Network Supporting Iranian Paramilitary Force That Recruits and Trains Child Soldiers."
27. UNSCR 2231 (July 2015) revises UN sanctions and other prohibitions, including financial prohibitions, concerning Iran. Financial institutions should be aware that the UN maintains a list of individuals and entities subject to targeted financial sanctions.
28. *See* FATF Public Statement (October 19, 2018).

In the case of the DPRK, existing U.S. sanctions and FinCEN regulations already prohibit any such correspondent account relationships, superseding the Section 312 obligations.

In the case of Iran, the Government of Iran and Iranian financial institutions remain persons whose property and interests in property are blocked under E.O. 13599 and section 560.211 of the Iranian Transactions and Sanctions Regulations. U.S. financial institutions and other U.S. persons continue to be broadly prohibited under the Iranian Transactions and Sanctions Regulations from engaging in transactions or dealings with Iran, the Government of Iran, and Iranian financial institutions, including opening or maintaining correspondent accounts for Iranian financial institutions; these sanctions impose obligations on U.S. persons that go beyond the obligations imposed under Section 312.

Reminder of General 312 Obligations

As a general matter, FinCEN reminds U.S. financial institutions of their duty to apply enhanced due diligence when maintaining correspondent accounts for foreign banks operating under a banking license issued by a country (1) designated as non-cooperative with respect to international anti-money laundering principles or procedures, by an intergovernmental group or organization of which the United States is a member, and with which designation the U.S. representative to the group or organization concurs, or (2) that has been designated as warranting special measures under Section 311.[29] The regulations implementing the Bank Secrecy Act, as amended by the USA PATRIOT Act, require covered financial institutions to ensure that their enhanced due diligence programs include, at a minimum, steps to:

- Conduct enhanced scrutiny of such correspondent accounts to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable law and regulation;
- Determine whether the foreign bank for which the correspondent account is established or maintained in turn maintains correspondent accounts for other foreign banks that use the foreign correspondent account established or maintained by the covered financial institution and, if so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks; and
- Determine, for any such correspondent account established or maintained for a foreign bank whose shares are not publicly traded, the identity of each owner of the foreign bank and the nature and extent of each owner's ownership interest.[30]

29. *See* 31 U.S.C. § 5318(i); 31 CFR §§ 1010.610(b) and (c) (Enhanced Due Diligence obligations for correspondent accounts established, maintained, administered or managed in the United States for certain foreign banks).

30. *Ibid*.

II. Jurisdictions Identified by the FATF as Having Strategic AML/CFT Deficiencies

The FATF publicly identifies jurisdictions with strategic AML/CFT regime deficiencies for which the jurisdictions have developed an action plan with the FATF. Consequently, these jurisdictions are included in the following list of jurisdictions with strategic AML/CFT deficiencies, as described in the FATF's "Improving Global AML/CFT Compliance: On-going Process."

Please click on each jurisdiction for additional information.

The Bahamas, Botswana, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen

Summary of Changes

Countries Added to the List

- The Bahamas, Botswana, and Ghana have been added to the list due to the lack of effective implementation of their AML/CFT framework. The Bahamas, Botswana, and Ghana have made high-level political commitments to work with the FATF and their respective FATF Style Regional Bodies to strengthen the effectiveness of their AML/CFT regimes, and to address any related technical deficiencies.

Review of Guidance Regarding Jurisdictions Having Strategic AML/CFT Deficiencies

U.S. financial institutions also should consider the risks associated with the AML/CFT deficiencies of the countries identified under this section (The Bahamas, Botswana, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen).[31] With respect to these jurisdictions, U.S. financial institutions are reminded of their obligations to comply with the due diligence obligations for FFIs under 31 CFR § 1010.610(a) in addition to their general obligations under 31 U.S.C. § 5318(h) and its implementing regulations.[32] As required under 31 CFR § 1010.610(a), covered financial institutions should ensure that their

31. This advisory updates previous FATF-related guidance on identified jurisdictions with AML/CFT deficiencies. Additional FinCEN guidance on Syria includes FIN-2013-A002 and FIN-2011-A010 as well as FIN-2011-A013, FinCEN's guidance on the Commercial Bank of Syria.

32. *See* generally 31 CFR §§ 1010.210: Anti-money laundering programs. Specific AML Program obligations are prescribed in 31 CFR §§ 1020.210 (Banks), 1021.210 (Casinos and Card Clubs), 1022.210 (Money Services Businesses), 1023.210 (Brokers or Dealers in Securities), 1024.210 (Mutual Funds), 1025.210 (Insurance Companies), 1026.210 (Futures Commission Merchants and Introducing Brokers in Commodities), 1027.210 (Dealers in Precious Metals, Precious Stones, or Jewels), 1028.210 (Operators of Credit Card Systems), 1029.210 (Loan or Finance Companies), and 1030.210 (Housing Government Sponsored Enterprises).

due diligence programs, which address correspondent accounts maintained for FFIs, include appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed in the United States. Such reasonable steps should not, however, put into question a financial institution's ability to maintain or otherwise continue appropriate relationships with customers or other financial institutions, and should not be used as the basis to engage in wholesale or indiscriminate de-risking of any class of customers or financial institutions. FinCEN also reminds financial institutions of previous interagency guidance on providing services to foreign embassies, consulates, and missions.[33]

Review of General Guidance

AML Program Risk Assessment: For the jurisdictions that were removed from the FATF listing and monitoring process, financial institutions should take the FATF's decisions and the reasons behind the delisting into consideration when assessing risk, consistent with their obligations under 31 CFR §§ 1010.610(a) and 1010.210.

Suspicious Activity Reports (SARs): If a financial institution knows, suspects, or has reason to suspect that a transaction involves funds derived from illegal activity or that a customer has otherwise engaged in activities indicative of money laundering, terrorist financing, or other violation of federal law or regulation, the financial institution must file a SAR.

SAR Filing Instructions: When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. **FinCEN further requests that financial institutions reference this advisory in the SAR narrative and in SAR field 35(z) (Other Suspicious Activity-Other) by including the following key term:**

"October 2018 FATF FIN-2018-A007"

to indicate a connection between the suspicious activity being reported and the countries and activities highlighted in this advisory.

SAR reporting, in conjunction with effective implementation of due diligence requirements and OFAC obligations by financial institutions, has been crucial to identifying proliferation financing as well as money laundering and terrorist financing. SAR reporting is consistently beneficial and critical to FinCEN and U.S. law enforcement analytical and investigative efforts, OFAC designation efforts, and the overall security and stability of the U.S. financial system.

33. *See* Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Interagency Advisory: Guidance on Accepting Accounts from Foreign Embassies, Consulates, and Missions," March 24, 2011; and Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Interagency Advisory: Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies, and Foreign Political Figures," June 15, 2004.

For Further Information

Additional questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov. Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.